

REMARKS/ARGUMENTS

Remarks Concerning Amendments to Claims

Claims 1 and 21 are amended. The added claim language is supported by Figs. 1-3 and pages 7-8 and 13 of the description.

Response to Claim Rejections — 35 USC § 103

Claims 1-3, 8-10 and 21 were rejected under 35 USC 103(a) as being unpatentable over US Patent Application Publication 2002/0032871 (hereinafter “Malan”) in view of US Patent Application Publications 2002/01011819 (hereinafter “Goldstone”).

Applicant responds by amending the claims and demonstrating how the amended claims are clearly distinct and patentable over Malan in combination with Goldstone. In particular, the claims are amended to specify that the claimed apparatus is connected between protected and unprotected sides of a network, that the claimed data packets are received from the unprotected side of the network, that the claimed TCP state transitions are transitions of the state of TCP connections through the apparatus, that the claimed valid TCP connections are TCP connections through the apparatus, and that the claimed layer 2, 3, 4 classification involves isolating header values and performing hierarchical protocol classification. These amendments limit the allowable interpretations of the claim language and clearly distinguish the claims from the teachings in the cited references.

Applicant notes for the record that, in the art of computer networking techniques and devices, the term “TCP state” has a well-defined and specific meaning. The *TCP Specification*, which is fundamental and very well-known among those skilled in the art, defines the TCP protocol as having a finite set of TCP states (one of which is the “ESTABLISHED state” recited in the claims). See, for example, page 21 of *RFC 793 - Transmission Control Protocol Specification* available at www.faqs.org/rfcs/rfc793.html. Thus, in the context of the present claimed invention, the only reasonable interpretation of the claimed TCP state transition is the clear and

well-established meaning of these terms within the art, i.e., a transition between one of the well-defined TCP states as defined by the TCP protocol.

In contrast with Malan's access control list (ACL), the claimed invention uses a table of legitimate IP addresses containing IP addresses which have established *valid TCP connections through the apparatus*. Thus, the IP addresses have the property of being based upon the established TCP connections through the apparatus. Moreover, in further contrast with Malan, the claimed invention involves adding an IP address to the table of legitimate IP addresses when the *TCP state of TCP connections through the apparatus transitions to "established" for the first time*. In other words, the table of IP addresses changes when the TCP state of TCP connections through the apparatus transitions.

Malan merely mentions the use of an access control list (ACL) as a filter mechanism, but does not teach that the ACL contains IP addresses which have established valid TCP connections through the apparatus, or adding an IP address to the ACL when the TCP state of TCP connections through the apparatus transitions. It is also significant to note that Malan describes an apparatus which receives information from routers and further instructs the routers with Access Control Lists to block the attack.

As for Goldstone, techniques are taught therein for DOS attack mitigation by detecting a DOS attack and alerting multiple routers of the address of the attack. However, Goldstone does not teach the specific claimed feature of maintaining a list of legitimate IP addresses that contains IP addresses which have established valid TCP connections through the apparatus, or the specific claimed feature of adding an IP address to the list when the TCP state of TCP connections through the apparatus transitions. Goldstone, therefore, does not teach the claimed limitations.

A further distinguishing feature is that the claimed apparatus is an edge device, i.e., it is positioned between protected and unprotected sides of a network. Malan and Goldstone, in contrast, do not teach this type of device.

Therefore, the cited references do not fairly teach or suggest the specific claimed features of the claims as amended. Moreover, as described in the specification, these features contribute to advantageous abilities to protect networks against unwanted attacks. Thus, the claims as amended are submitted to be patentable over the references of record.

In view of the above, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

/ Thomas J. McFarlane /

Thomas J. McFarlane, Reg. No 39,299

LUMEN PATENT FIRM
2345 Yale Street, Second Floor
Palo Alto, CA 94306
(650) 424-0100